IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF NEW MEXICO

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
	)	Criminal No. 16-04571 JCH
vs.	)	
	)	
GUY ROSENSCHEIN,	)	
	)	
Defendant.	)	

UNITED STATES' SURREPLY REGARDING DEFENDANT'S MOTION FOR DISCLOSURE OF EXPERT REPORTS (DOC. 212)

The United States submits this surreply in opposition to Defendant's Reply in Support of his Motion for Disclosure of Expert Reports. Doc. 212. In his reply, Defendant expands the scope of his initial request and mischaracterizes the anticipated testimony of the United States' witnesses. With leave of the Court, Doc. 237, the United States submits this surreply and renews its request for the Court to deny Defendant's motion.

DISCUSSION

In his reply in support of his motion for expert reports, Defendant continues to move the goalposts by lodging additional, expansive discovery requests, and mischaracterizing the expected testimony from the United States' witnesses. These tactics only serve to further undermine Defendant's position. The fact remains that Mr. Shehan and Mr. Lilleskare are not expert witnesses, and Defendant is not entitled to Rule 16(a)(1)(G) discovery. Further, Defendant's reply represents a blatant attempt to circumvent the Court's prior rulings on the same discovery requests, as well as his agreement with Microsoft to forgo an additional subpoena for this precise material. In any event, Defendant is not entitled to the requested material because he has failed to establish how these items would further his agency theory,

other than pointing to speculative arguments. For these reasons, the Court should deny Defendant's motion.

I. Defendant's attempt to reframe the anticipated testimony of United States' witnesses does not recast them as experts.

In support of his position that Mr. Shehan and Mr. Lilleskare are expert witnesses, Defendant mischaracterizes the scope of the witnesses' anticipated testimony. Each witness has filed two declarations in response to the issues raised by Defendant in his suppression motions. Docs 86-2, 94-1 (Lilleskare); Docs. 72-1, 94-2 (Shehan). Despite this, Defendant claims that the witnesses will offer highly technical testimony that falls outside the knowledge of an "ordinary person." Doc. 231 at 8. Microsoft recently explained that Defendant appears to be operating under a "fundamental misunderstanding of the testimony that Mr. Lilleskare is prepared to provide." Doc. 242-1 at 6. Mr. Lilleskare does not have "technical expertise" regarding the PhotoDNA algorithm, only a "working knowledge" of PhotoDNA functions. *Id.* at 7. Further, with respect to Mr. Shehan, NCMEC has indicated that he is able to testify regarding "any information in NCMEC's possession that could conceivably be relevant to Rosenschein's Motion to Suppress." Doc. 211 at 5. The level of detail necessary to litigate Defendant's suppression motions is consistent with the scope of knowledge possessed by the United States' witnesses. This knowledge is fairly characterized as relating to the business and service operations of their respective companies. *See* Doc. 220 at 9. Defendant's desire to cross-examine the United States' witnesses on matters outside their purview, and beyond the scope of his motions, does not transform these individuals into expert witnesses.

II. Defendant's new discovery request is contrary to the Court's denial of his prior attempts to obtain this material.

In his reply, Defendant requests, for the first time, that the United States produce proprietary source code as part of his request for expert discovery material. This request is nothing more than an attempt to circumvent prior, unsuccessful attempts to procure this same, sensitive information. First, Defendant attempted to obtain material relating to Microsoft's PhotoDNA software and "API reporting program" in his Federal Rule of Criminal Procedure 17(c) subpoena to Microsoft. Following litigation over the scope of this subpoena, the Court denied Defendant's request for this material. Doc. 199 at 11-12. Second, despite this ruling, Defendant reached out to Microsoft and requested additional information beyond the scope of the Court's order. Doc. 242-1 at 4. In the course of this communication, Defendant ultimately agreed not to pursue an additional Rule 17(c) subpoena that would request production of Microsoft's PhotoDNA algorithm. Doc. 242-1 at 4-5. Third, Defendant attempted to obtain "access credentials to the PhotoDNA algorithm or the PhotoDNA algorithm itself as well as any associated API" through Gregory Clark, a Microsoft witness he subpoenaed pursuant to Federal Rule of Criminal Procedure 17(a). The Court referred Microsoft's motion to quash this subpoena to Judge Ritter, who expressly recommended that the witness not be required to bring PhotoDNA access credentials to the hearing. Doc. 189 at 11. In this Court's final ruling on the motion to quash, the Court accepted Judge Ritter's recommendations with respect to Mr. Clark. Doc. 203.

Now, under the guise of a request for expert reports, Defendant again attempts to obtain this same, sensitive material, this time from the United States. It should not be lost on the Court what is actually going on here—a graymailing-type attempt to forestall this prosecution. *United States v. Abu Ali*, 528 F.3d 210, 245 (4th Cir. 2008) (graymailing is a "practice whereby a criminal defendant threatens to reveal classified information during the course of his trial in the

hope of forcing the government to drop the charge against him.") (citation omitted). Defendant is violating his own agreement with Microsoft and attempting to circumvent two separate rulings by the Court denying his requests for the same material. The Court should not reward these tactics by granting Defendant's improper discovery requests.

III. Even if the Court treats this as a properly-lodged discovery request, Defendant has failed to establish the relevance of the requested material.

Even if the Court elects to treat these witnesses as experts, and entertain Defendant's discovery request, highly sensitive source code far exceeds anything reasonably contemplated in an expert report pursuant to Rule 16(a)(1)(G). Various courts have examined discovery requests for source code and regularly concluded that it is not material to the defense. Although many of the courts also point to law enforcement privilege as a secondary basis for denial, the materiality analysis remains relevant and instructive. *See, e.g. Jean v. United States*, 891 F.3d 712, 715 (8th Cir. 2018) (upholding denial of defendant's request for disclosure of complete source code for the software used to identify him, where likelihood it would help his defense was "vanishingly small"); *United States v. Kienast*, 907 F.3d 522, 530 (7th Cir. 2018) (upholding a denial of defense request for source code as immaterial and "essentially a fishing trip"); *United States v. French*, 2010 WL 1141350, at *4 (D. Nev. 2010) (breathalyzer source code not discoverable because not in government's possession); *United States v. Dillow*, 980 F.Supp.2d 879, 883 (N.D. Ohio 2013) (denying defendant's request for disclosure of software program used by state law enforcement when not in the possession of the United States Attorney's Office). These cases demonstrate that courts should—and do—exercise their gatekeeping function to rein in immaterial, expansive discovery requests. In any event, as in *French* and *Dillow*, the United States is not in possession of the proprietary material requested by Defendant.

Here, Defendant has failed to establish how the requested items would further his argument that Microsoft is an agent of NCMEC—his attempts at justifying this request are premised on nothing more than gross speculation. Defendant inexplicably claims that the United States' witnesses are going to lie under oath and therefore the requested source code is necessary to impeach them. The reality is that Defendant is already in possession of well beyond what Rule 16 requires and what is necessary to mount his defense. The United States has produced voluminous discovery, including the CyberTipline Reports in question and identification of the available hash match sources. Additionally, both NCMEC and Microsoft have produced extensive material in response to Defendant's Rule 17(c) subpoenas and the Court's subsequent rulings. *See* Doc. 183 at 11 (Judge Ritter noting that Microsoft provided "more than the Court would otherwise require.").

With respect to the hash sources utilized by PhotoDNA during the timeframe of the charged offenses, the United States previously disclosed that the hash match in this case was made by the database shared by NCMEC and its Canadian counterpart, Cybertip.ca. Doc. 175 at 9. Although there is no "receipt", so to speak, for this match, the United States understands that Mr. Shehan will be able to identify the hash source, speak to the reliability of the hash database, and confirm that the hash values for both of the distributed images were in the database prior to Chatstep flagging the material on its server. While Defendant claims that he needs the actual source code to cross-examine the witnesses on these topics, he has not linked how the algorithm would put him in a position to conduct this cross-examination.

CONCLUSION

For the foregoing reasons, the United States urges the Court to deny Defendant's motion for expert reports.

Respectfully submitted,

JOHN C. ANDERSON
United States Attorney

Electronically filed June 12, 2020
SARAH J. MEASE
HOLLAND S. KASTRIN
Assistant United States Attorneys
P.O. Box 607
Albuquerque, N.M. 87103

I HEREBY CERTIFY that the foregoing pleading was filed electronically through the CM/ECF system, which caused counsel of record for Defendant to be served by electronic means.

/s/
SARAH J. MEASE
Assistant United States Attorney